Le leader de la logistique Simon Hegele sécurise ses terminaux mobiles et établit une conformité RGPD

Profil du client

Le leader allemand de la logistique Simon Hegele propose des solutions internationales d'achat, de production et de conditionnement, ainsi qu'une logistique dédiée aux pièces de rechange et une gestion de la sécurité des chaînes d'approvisionnement dans les secteurs de la vente au détail, de la santé et de l'informatique/communication.

Secteur d'activité : Logistique

Politique de mobilité : COPE

Solution EMM : MobileIron

La solution : Lookout Mobile Endpoint Security

Les résultats : Conformité aux exigences du RGPD, utilisation sans risque des données d'entreprise

Le défi

Depuis sa création en 1920, le fournisseur mondial de services logistiques Simon Hegele a fait du chemin. Constituée au départ de deux chevaux et d'une cariole, l'entreprise originelle de transport de marchandises est devenue un leader mondial qui propose aujourd'hui des services à valeur ajoutée très spécialisés, adaptés aux processus de ses clients. Comptant 2 500 employés répartis sur 49 sites différents dans le monde, l'organisation a elle aussi ses propres défis et doit notamment trouver comment continuer à assurer la protection et la conformité de ses effectifs mobiles et de ses données d'entreprise.

Confrontés aux nouvelles réglementations de conformité avec le RGPD, à une hausse des risques liés aux appareils mobiles et aux complexités associées à la mise en œuvre d'une politique de mobilité contrôlée par les entreprises, les chefs d'entreprise ont opté pour une solution de sécurité mobile globale.

Défis de la sécurité

- Bénéficier d'une protection et d'un support en temps réel pour les points de terminaison mobiles au sein d'un environnement Android et iOS
- Protéger les données d'entreprise contre les points de terminaison mobiles compromis
- Respecter les nouvelles réglementations prévues par le Règlement général sur la protection des données (RGPD)

Simon Hegele attribue sa réussite des 90 dernières années à l'implication, au dévouement et à la passion de ses employés. Une solution aux politiques restrictives ou chronophages et aux exigences complexes n'était pas envisageable. « Notre partenaire de confiance, anyplace IT GmbH, nous a conseillé Lookout en soulignant que la solution pouvait répondre à nos besoins grandissants en matière de sécurité mobile, tout en s'intégrant à notre plate-forme EMM MobileIron sans imposer de contraintes supplémentaires à nos employés », explique Christian Jösch, administrateur réseau chez Simon Hegele.

La solution

Pour répondre à ses besoins en matière de sécurité mobile, l'entreprise a opté pour Lookout Mobile Endpoint Security. L'approche adoptée pour le déploiement consistait à utiliser la plate-forme EMM MobileIron en vue de déployer l'application Lookout for Work sur les appareils mobiles des employés. « Le déploiement s'est très bien déroulé », affirme Christian Jösch. « Tous les appareils de notre parc mobile sont désormais protégés contre les menaces et les risques, tels que les attaques de type man-in-the-middle, les applications sideloadées et les logiciels malveillants. »

Avec Lookout Mobile Endpoint Security, les employés peuvent désormais se connecter aux ressources d'entreprise en toute sécurité, partout dans le monde. En outre, grâce à l'accès à des fonctionnalités personnalisables de contrôle de la confidentialité, le respect des exigences du RGPD relatives au traitement des données des utilisateurs constitue désormais un processus simple et intuitif.

« Nous considérons la sécurisation des terminaux mobiles comme une priorité absolue. Lookout nous sert de couche de protection stratégique, non seulement pour éviter que les données de notre entreprise ne soient compromises, mais aussi pour veiller à leur conformité avec les lois relatives au respect de la vie privée », affirme Christian Jösch.

Les résultats

Dès son déploiement, Lookout Mobile Endpoint Security a eu des retombées inattendues. « Nous étions surpris », explique Christian Jösch, « par le nombre de menaces, et notamment de riskware et d'attaques de type man-in-the-middle, détecté sur les appareils de nos employés qui comprenaient également des données d'entreprise. À l'aide d'une analyse en temps réel et de l'avantage que présente l'ensemble de données mobile unique de Lookout, nous avons corrigé ces menaces et disposons à présent d'une visibilité complète sur les nouvelles menaces qui nous intéressaient. »

Plus important encore, l'entreprise a acquis la capacité à se conformer aux nouvelles réglementations plus strictes en matière de protection de la vie privée. Alors que de nombreuses organisations ont préparé des points de terminaison traditionnels pour se conformer aux exigences du RGPD, la mobilité présente des défis de sécurité uniques et complexes. Étant donné que les employés d'aujourd'hui ont la possibilité de choisir les appareils, les applications et les réseaux à partir desquels accéder aux données et aux applications d'entreprise, le spectre des risques mobiles prend de plus en plus d'ampleur. Avec Lookout Mobile Endpoint Security, Simon Hegele est tout à fait en mesure de se prémunir contre la compromission des données liée aux attaques malveillantes et aux fuites de données non malveillantes, et peut également étendre ses contrôles de sécurité mobile à la protection de ses données personnelles.

Cette collaboration aura permis à l'entreprise d'atteindre tous ses objectifs en matière de sécurité mobile et de conformité. Grâce à la sécurité intégrée des terminaux mobiles, aux fonctionnalités de conformité RGPD personnalisables et à l'analyse en temps réel des nouvelles applications et des versions d'applications des appareils, l'entreprise est parée à poursuivre sa croissance historique en toute confiance en proposant des services et des solutions de classe mondiale à ses clients.

Critères de la solution

- Doit pouvoir protéger les appareils Android et iOS des menaces réseau et applicatives, y compris des riskware et des logiciels malveillants
- Doit permettre aux effectifs mondiaux de l'entreprise de se connecter de façon sécurisée au réseau de l'entreprise
- Doit s'intégrer en toute transparence à MobileIron, la plate-forme EMM de l'organisation, et être simple d'utilisation pour les employés
- Doit proposer une analyse des appareils en temps réel afin de protéger la sécurité et la confidentialité des employés et des données d'entreprise

> « Le déploiement s'est très bien déroulé… Tous les appareils de notre parc mobile sont désormais protégés contre les menaces et les risques, tels que les attaques de type man-in-the-middle, les applications sideloadées et les logiciels malveillants. »

Christian Jösch,
Administrateur réseau
Simon Hegele